

Professor Catherine Sandoval
Reply Comments, WC Docket No. 17-108
Exhibits A, B and C

Attached to my Reply Comments as Exhibit A is a true and correct copy of the May 25, 2017 letter from Fight for the Future which alleges that the names and addresses of the persons signing the letter were used without their permission to file comments in the FCC's Internet Freedom Rulemaking.

Attached as Exhibit B is a true and correct copy of the June 28, 2017 letter from Congressman Pallone to the Honorable Jefferson Sessions requesting that the U.S. Department of Justice launch an investigation of the alleged identity theft and comments filed based on alleged database breaches in the FCC Internet Freedom docket.

Attached as Exhibit C is a true and correct copy of the Op Ed I wrote dated May 19, 2017, Protect the Open Internet, published by the Daily Journal.

I, Catherine J.K. Sandoval, certify under penalty of perjury that these are true and correct copies of the documents attached hereto as Exhibits A, B, and C.

Dated: August 30, 2017

A handwritten signature in black ink, appearing to read "Catherine J.K. Sandoval", written in a cursive, flowing style.

<https://www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and/>

Letter to the FCC from people whose names and addresses were used to submit fake comments against net neutrality

Posted 10:40 EDT on May 25, 2017

May 25, 2017
The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dr. David A. Bray
Chief Information Officer
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

CC Members of U.S. Congress

Dear Chairman Pai,

Our names and personal information were used to file comments we did not make to the Federal Communications Commission.

We are disturbed by reports that indicate you have no plans [1] to remove these fraudulent comments from the public docket. Whoever is behind this stole our names and addresses, publicly exposed our private information without our permission, and used our identities to file a political statement we did not sign onto. Hundreds of thousands of other Americans may have been victimized too.

We call on you, the Chairman of the Federal Communications Commission, to take the following actions:

- Notify all who have been impacted by this attack
- Remove all of the fraudulent comments, including the ones made in our names, from the public docket immediately
- Publicly disclose any information the FCC may have about the group or person behind the 450,000+ fake comments
- Call for an investigation by the appropriate authorities into possible violations of 18 U.S.C. § 1001 ("making false statements") and other relevant laws.

As chairman of the FCC, an independent federal agency, it is your responsibility to maintain public trust, especially while your agency is fielding comments on the future of the free and open Internet, an issue that millions of Americans care deeply about.

Based on numerous media reports [2], nearly half a million Americans may have been impacted by whoever impersonated us in a dishonest and deceitful campaign to manufacture false support for your plan to repeal net neutrality protections.

While it may be convenient for you to ignore this, given that it was done in an attempt to support your position, it cannot be the case that the FCC moves forward on such a major public debate without properly investigating this known attack.

All proper authorities must be notified immediately and the FCC must disclose any and all information the agency has pertaining to the organization or person behind these fake comments.

Sincerely,

Brittany Ainsworth, Huntington Beach, CA
Greg Baynes, View Park, CA,
William Brahams, San Bernardino, CA
Christian Brown, Redondo Beach, CA
John Burr, New York, NY
Angelica Collins, Bear, DE
Megan Conschafter, Buffalo, NY
Ben Currier, Littleton, CO
Norman Daoust, Cambridge, MA
Cynthia Duby, Desert Hot Springs, CA
Aaron Francis, Santa Ana, CA
Michelle Ellett, Benicia, CA
Adam Galatioto, Gainesville, FL
Surbhi Godsay, Nashua, NH
Daniel Hickey, Worcester, MA
Richard O. Johnson, Castro Valley, CA
Samuel Lewis, Oakland, CA
Paulo Llanes, Seattle, WA
Joel Mullaney, Watertown, MA
Shaun O'Brien, Elito, ME
Nicholas Pannuto, Sterling Heights, MI
Daniel Pinkert, New York City, NY
John Ulick, Champaign, IL
Arianna Williams, Philadelphia, PA
Melissa Williams, Dallas, TX
Nicholas Ryan, East Lansing, MI
Adam Stone, Salt Lake City, UT

[1] <http://www.vocativ.com/431065/fcc-ajit-pai-net-neutrality-bots/>

[2] <https://www.theverge.com/2017/5/10/15610744/anti-net-neutrality-fake-comments-identities>

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 28, 2017

The Honorable Jefferson B. Sessions III
Attorney General
U.S. Department of Justice
950 Pennsylvania Ave, NW
Washington, D.C. 20530

Mr. Andrew G. McCabe
Acting Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20530

I write to urge you to investigate whether federal law has been violated by the submission of fake comments to the Federal Communications Commission (FCC) using stolen identities.

This request comes after troubling reports that 14 people recently alerted the FCC that their names and addresses had been used to file net neutrality comments without their knowledge or permission.¹ Reports also indicate that 450,000 identically drafted comments have been filed in the FCC's open internet docket by an unknown party.² Other reporting suggests that the persons filing these fake comments may be using information obtained from data breaches.³

¹ Letter from 14 Persons to FCC Chairman Ajit Pai and FCC CIO David Bray (May 25, 2017) (www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and/).

² *People Who Were Impersonated by Anti-Net Neutrality Spammers Blast FCC*, ARS Technica (May 25, 2017) (arstechnica.com/information-technology/2017/05/identity-theft-victims-ask-fcc-to-clean-up-fake-anti-net-neutrality-comments/).

³ *The Anti-Net Neutrality Bot Spamming the FCC is Pulling Names from Leaked Databases*, The Verge (May 11, 2017) (www.theverge.com/2017/5/11/15626278/net-neutrality-spam-bot-fcc-leak-data).

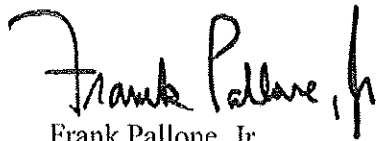
The Honorable Jefferson B. Sessions III
Mr. Andrew G. McCabe
June 28, 2017
Page 2

These parties may be attempting to influence federal policy by publicly misrepresenting the views of innocent victims. As part of its online comment filing system, the FCC is also publicly listing these victims' private information, including their addresses, making this situation more urgent.

Federal law prohibits knowingly making any materially false statement or representation in any matter within the jurisdiction of the executive, legislative, or judicial branch.⁴ I am deeply concerned that the sheer number of these potentially false comments suggest a coordinated attempt to materially mislead the FCC, and therefore a coordinated attempt to break federal law. I urge you to take swift action to investigate who may be behind these comments and, if appropriate under applicable federal law and regulations, prosecute the people behind these fraudulent comments.

I appreciate your attention to this important request and ask that you provide me and my staff an update on your progress pursuing this matter one month from today on July 28. If you have any questions, please contact the minority committee staff at (202) 225-3641.

Sincerely,

A handwritten signature in black ink that reads "Frank Pallone, Jr." with a stylized flourish at the end.

Frank Pallone, Jr.
Ranking Member

⁴ 18 U.S.C. 1001.

Daily Journal

www.dailyjournal.com

FRIDAY, MAY 19, 2017

Protect the open internet

By Catherine J.K. Sandoval

Imagine an internet where your internet service provider (ISP) could enter into undisclosed deals to speed up select content or block legal sites based on the ISP's business interests. The Federal Communications Commission and the U.S. Court of Appeals for the D.C. Circuit in *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), recognized that ISPs have both the financial incentive and technical ability to engage in paid prioritization. Such deals are barred by FCC "Open Internet" rules adopted in 2015, but FCC Chairman Ajit Pai proposes to repeal those rules. His proposal asks whether ISPs should be allowed to manage internet networks based on their own business justifications, and whether industry self-regulation or voluntary promises are preferable to enforceable FCC rules. All Americans should be concerned about this proposal's implications for democracy, the economy, security and competition.

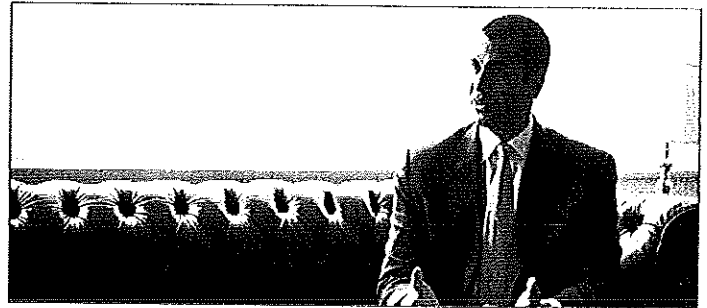
Self-regulation and voluntary policies provide no recourse in contract law and may not be enforceable under the FCC's proposal. Many major ISPs post policy statements on their websites proclaiming that the ISP does not block or throttle data, but these policies are excluded from their consumer contracts. These statements are neither written in the language of promise nor condition, nor are they integrated into user agreements, rendering them unenforceable in contract. Verizon lists in its terms of service page a hyperlink to its "Open Internet Policy." Clicking on that hyperlink leads to a message "Access Denied, You are not authorized to access this page." We can only hope that this link was accidentally broken and that Verizon soon restores public access to its open internet policy highlighted in its terms of service.

Even if ISPs included no blocking, throttling or paid prioritization promises in their contracts, most ISPs reserve the right to modify their internet service contract at their discretion and contend that continued use of the service constitutes agreement. The FCC found that most Americans have only one or two choices for wireline high-speed internet providers, and many wireless services impose data caps. Internet users lack a competitive market in which to shop

around restrictive contract terms or policies. The FCC proposal would repeal the requirement that ISPs interconnect their network to competitors, rendering competition less likely. The proposed rollback of the open internet rules doesn't require ISPs to extend or build networks, or create sufficient incentives to do so, particularly in higher cost rural and mountainous areas.

The FCC asks whether we should rely on antitrust laws instead of bright-line rules to deter internet blocking, throttling or paid prioritization. The prospect of antitrust enforcement deters some anti-competitive conduct, but may not be sufficient or timely to prevent harms to competition and innovation. Internet service providers could raise rivals' costs to the detriment of small or independent publishers, producers and others who use the internet to distribute content that competes with the services of the ISP or its affiliates. Repeal of ex ante discrimination rules would add to questions about whether a merger increases the ISPs' ability and incentive to engage in anticompetitive behavior. The Federal Trade Commission Act prohibits unfair and deceptive trade practices — duplicity in advertising that harms competitors or consumers. The FTC act does not confer jurisdiction to adopt forward looking rules such as the FCC's open internet protections.

Antitrust and unfair competition laws provide a remedy for antitrust-injury type harms to competition, but not for public interest harms. How can we safeguard our democracy, economy and national interest if no rules or laws prohibit ISP blocking, data throttling or paid prioritization and ISPs drop their voluntary policies not to engage in such practices? Could the messages of American families, businesses, church and civic organizations, or government agencies be muted by fast lane deals offered to some deep-pocket entities, but not to all? What happens to our democracy if candidates for political office or their supporters, domestic or foreign, could enter into undisclosed special deals for fast internet access or thwart contesting messages? Media deals once done through personal relationships are now often done online. When I was the General Counsel for Z-Spanish Media Company in the early 2000s, I knew the buyer for McDonalds who sought to place ads on our Spanish and English



Ajit Pai in his office in Washington, D.C., Aug. 16, 2013.

New York Times News Service

language radio stations and websites. Could repeal of the FCC's open internet protections enable online deals to speed or prioritize internet traffic or block other user's data, even if the highest bidder represents foreign interests? We need legally enforceable open internet rules to protect American democracy and our national interests.

Many ISPs publicly state that they support an open internet but argue for repeal of the FCC's 2015 rules that classified ISPs as common carriers under Title II of the Communications Act. Internet service provider Verizon led the charge in *Verizon* against the FCC's 2010 broadband framework that prohibited blocking and throttling under Title I of the Communications Act and Section 706 of the Telecommunications Act of 1996. The *Verizon* decision overturned the FCC's 2010 rules on the grounds that they imposed common carrier-like nondiscrimination obligations characteristic of Title II without adopting Title II as the legal basis for those rules.

Following the *Verizon* decision, the FCC 2015 open internet proceeding asked whether the FCC should allow ISPs to engage in individualized bargaining for private and potentially exclusive fast-lane deals, or whether ISPs should be classified as common carriers. While serving as a commissioner of the California Public Utilities Commission, I filed comments in that proceeding highlighting the crucial role of the open internet rules for public safety, public health, national security and critical infrastructure such as electric, water, gas and communications services. Electric and gas utilities use the internet to ask customers to reduce demands on the electric grid to prevent blackouts, or locate natural gas leaks. The open internet allowed a California inventor to develop a technology to detect gas leaks at a rate 1000 times more sensitive than previous methods. Such innovation requires that

all Americans have access to an open internet. The FCC decided in 2015 that ISPs were engaged in common carrier activity, and that Title II classification was appropriate to protect the open internet. The D.C. Circuit last year upheld the FCC's 2015 open internet rules, and this year declined to rehear that case en banc, based on *Chevron* deference to the FCC's judgment that the open internet rules protect the virtuous cycle of innovation internet access enables.

The internet is essential to our economy, services and security, and is increasingly the town square of democracy. It enables health care information and monitoring to extend from the doctor's office to the home, making open internet access at home crucial to health, safety and controlling health care costs. President Donald J. Trump's executive order on cybersecurity and critical infrastructure adopts "an open, interoperable, reliable, and secure internet" as the policy of the executive branch. The FCC's proposal to rollback open internet protections undermines the president's policies and the internet's power to spur our economy, and safeguard our democracy. We need legally enforceable rules to protect access to the open internet. The FCC's 2015 open internet rules do just that and merit continued support.

Catherine J.K. Sandoval is a professor at Santa Clara University School of Law where she teaches contract, communications, antitrust and energy law. She served as a commissioner of the California Public Utilities Commission from January 2011 to January 2017.

